AF/2131
83

OIPE JUN 21 2004 PATENT & TRADEMARK OFFICE

Practitioner's Docket No. NAI1P263/99.010.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

re application of: Glen Sonnenberg

Application No.: 09/471,630 Group No.: 2131
Filed: 12/24/1999 Examiner: Jackson, Jenise
For: SYSTEM AND METHOD FOR SELECTIVE COMMUNICATION SCANNING AT A FIREWALL AND A NETWORK NODE

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED
JUN 24 2004
Technology Center 2100

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 27, 2004.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

✓ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
✓ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

_ facsimile transmitted to the Patent and Trademark Office, (703) _____ - _____

Erica L. Farlow
Signature

Date: 6/18/04

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity $330.00

Appeal Brief fee due $330.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$330.00
Extension fee (if any)	$0.00

TOTAL FEE DUE $330.00

6. FEE PAYMENT

Attached is a check in the amount of $330.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P263).

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Silicon Valley IP Group, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity	$330.00

Appeal Brief fee due $330.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$330.00
Extension fee (if any)	$0.00

TOTAL FEE DUE $330.00

6. FEE PAYMENT

Attached is a check in the amount of $330.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P263).

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Silicon Valley IP Group, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
Sonnenberg et al.	) Group Art Unit: 2131
Application No. 09/471,630	) Examiner: Jackson, Jenise E.
Filed: 12/24/99	) Date: June 18, 2004
For: SYSTEM AND METHOD FOR SELECTIVE COMMUNICATION SCANNING AT A FIREWALL AND A NETWORK NODE	)

Commissioner for Patents
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on May 27, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. § 1.192(a))

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 1.192(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF INVENTION

VI ISSUES

VII GROUPING OF CLAIMS

VIII ARGUMENTS

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 1.192(c)(1))

The real party in interest in this appeal is Networks Associates Technology, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 1.192(c)(2))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals or interferences.

III STATUS OF CLAIMS (37 C.F.R. § 1.192(c)(3))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-22.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration but not canceled: None
2. Claims pending: 1-22
3. Claims allowed: None
4. Claims rejected: 1-22

C. CLAIMS ON APPEAL

The claims on appeal are: 1-22

IV STATUS OF AMENDMENTS (37 C.F.R. § 1.192(c)(4))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF INVENTION (37 C.F.R. § 1.192(c)(5))

In one embodiment, a system and methods are provided for scanning a communication that is received at a firewall on behalf of a destination node on one or the other of the firewall and the destination node. See Figure 1B. In particular, a set of rules, criteria or parameters may be established to determine when a communication is to be scanned for target content (e.g., computer viruses, programming objects, content of a particular type) on a destination node instead of the firewall. Note operation 516 of Figure 5 and the accompanying description. Overall performance of the firewall may thus be enhanced by off-loading some of its communication scanning responsibilities to a trusted host or node that is connected to the firewall.

VI ISSUES (37 C.F.R. § 1.192(c)(6))

Issue # 1: The Examiner has rejected Claims 1-22 under 35 U.S.C. §102(e) as allegedly being anticipated by Segal (6,345,299).

VII GROUPING OF CLAIMS (37 C.F.R. § 1.192(c)(7))

The claims of the following groups do not stand or fall together. Following is the grouping of claims. In the following section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1: Grouping of Claims

Group #1: Claims 1-2, 9, 10-11, and 13-21

Group #2: Claim 3

Group #3: Claims 4 and 5

Group #4: Claim 6

Group #5: Claim 7

Group #7: Claim 8

Group #8: Claim 12

Group #9: Claim 22

VIII ARGUMENTS (37 C.F.R. § 1.192(c)(8))

Issue #1:

The Examiner has rejected Claims 1-22 under 35 U.S.C. §102(e) as allegedly being anticipated by Segal (6,345,299).

Group #1: Claims 1, 9, 10-11, and 13-21

With respect to Group #1, Appellant respectfully disagrees with such rejection, since the Examiner's sole reference fails to meet each of appellant's independent claim limitations.

The Examiner continues to rely on the following excerpt from Segal to make a prior art showing of appellant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" (see Claims 1 and 17), "a set of criteria to be applied to said communication to determine if said communication is to be scanned for target content at the firewall or at the destination node" (see Claim 18), and "a set of rules configured to determine whether said communication is to be scanned for said target content on said firewall or on the first node" (see Claim 19).

> "In accordance with the invention, the network 40 the units 43, 45, 46, 47, 49, and 50 each comprise a shared list setting forth a plurality of listed nodes and a set of access privileges for each listed node. Access privileges are the types of transmissions that a given node listed in the shared list is permitted to make. For example, consider the case where node B1 is a computer or LAN at an accounting firm. The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 2, line 60 - col. 3, line 15)

Specifically, with respect to appellant's claimed "maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall" (emphasis added), the Examiner points out the foregoing discussion of the exemplary use of the shared list in Segal, and then concludes "Segal discloses that the node and the firewall communicate to determine which transmissions are to be transmitted."

Even if the Examiner's conclusion summary accurately describes what Segal discloses, it still fails to meet all of appellant's claim limitations. In the Examiner's cited example above, the node B1 is not capable of any scanning, thus there is clearly no disclosure, teaching or even suggestion of any sort of determining when one of said communications **may be scanned at a computer node** connected to the firewall **instead of at the firewall**. Only appellant teaches and claims such specific interplay between a computer node and a firewall, whereby scanning occurs on one or the other based on a set of criteria.

The Examiner continues by stating that Segal inherently discloses a virus scanner, in view of the excerpt from Segal below:

> "The situation can be improved upon by providing a set of firewall-type commands that include lists of which nodes, sources, networks are allowed to use certain destinations. These commands can be utilized by filtering devices and/or security devices such as firewalls, ingress

nodes, switches, which would be informed which destination nodes, addresses, ports, are permitted to which source nodes or networks. These filtering devices and/or security devices may be separate stand-alone components or their capability may be integrated into other, possibly already existing, devices." (col. 3, lines 35-45)

Further, the Examiner concludes that "Segal discloses a firewall that filters and scans data." First, appellant notes that there is no mention of "scanning" in Segal. Moreover, even if there were some sort of scanning inherently disclosed in Segal, it would still fail to meet appellant's claimed "virus scanner" feature.

Appellant asserts that the disclosure of a firewall does not necessarily meet the limitation of a "virus scanner," neither explicitly nor implicitly. See, for example, an illustrative definition of a firewall, indicating the broadest plain and ordinary meaning thereof.

"firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted."

http://www.webopedia.com/TERM/f/firewall.html

There is simply no mention of any sort of virus scanning in such definition. Appellant further brings the Examiner's attention to what is well known in the computer industry, namely virus scanner and firewall products/features are separate entities which, may be used in combination, but are nevertheless functionally different. Again, the Segal reference fails to meet appellant's claims.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Segal reference, in view of the arguments set forth hereinabove.

Group #2: Claim 3

With respect to Group #2, the Examiner relies on the following excerpt from Segal to make a prior art showing of appellant's claimed "marking said second communication before said forwarding to said second computer node."

> "The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4…" (col. 3, lines 1-7)

Such excerpt from Segal and the remaining Segal reference, however, merely suggests a "shared list" that "intercept[s] all e-mail and only allow[s] e-mail from [certain] nodes." Thus, the shared

lists appears to simply track certain nodes, and there is simply no disclosure, teaching or even suggestion of any sort of "marking said second communication before said forwarding to said second computer node" (emphasis added).

Again, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #3: Claims 4 and 5

With respect to Group #3, the Examiner relies on the following excerpts from Segal to make a prior art showing of appellant's claimed:

"wherein said partitioning comprises:

receiving scanning capabilities of a first computer node connected to the firewall;

consulting a set of scanning requirements specified by an operator of the firewall; and

specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node."

"In accordance with the invention, the network 40 the units 43, 45, 46, 47, 49, and 50 each comprise a shared list setting forth a plurality of listed nodes and a set of access privileges for each listed node. Access privileges are the types of transmissions that a given node listed in the shared list is permitted to make. For example, consider the case where node B1 is a computer or LAN at an accounting firm. The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 2, line 60 - col. 3, line 15)

Simply nowhere in such excerpt from Segal is there any disclosure, teaching or even suggestion of any sort of "receiving scanning capabilities of a first computer node connected to the firewall" and "consulting a set of scanning requirements specified by an operator of the firewall" and "specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node." Again, as set forth hereinabove, Segal discloses no "scanning," let alone receiving scanning capabilities, consulting a set of specified scanning requirements and further specifying a set of criteria to identify when a communication may be scanned for target content. It is noted that Segal suggests criteria for conditionally blocking e-mails, not criteria for conditionally scanning for target content.

Again, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #4: Claim 6

With respect to Group #4, the Examiner has simply dismissed the subject matter of Claim 6 by stating that such limitations have already been discussed with respect to Claim 1. Appellant respectfully disagrees.

Just by way of example, the Examiner has not addressed, at the very least, the following emphasized limitations of Claim 6:

> "identifying whether said firewall is capable of scanning said first communication for target content;
>
> determining whether said firewall is configured to share responsibility for scanning said communications with one or more of said plurality of computer nodes;
>
> determining whether said first node is capable of scanning said first communication for said target content; and
>
> determining whether said communication satisfies one or more criteria in said set of criteria."

Again, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #5: Claim 7

With respect to Group #5, the Examiner states that the limitations of Claim 7 have already been addressed by the Examiner during the application of Segal to Claims 1-2. Appellant respectfully disagrees. Just by way of example, the Examiner has not addressed, at the very least, the following emphasized limitations of Claim 7:

"maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and when said communication may be scanned by the destination node of said communication;

receiving a first communication at the firewall, wherein said first communication is intended for a first computer node connected to the firewall;

determining whether a first virus scanner is enabled on the firewall;

determining whether a second virus scanner is enabled on said first computer node;

identifying a first set of attributes of said first communication;

determining from said first set of attributes and said rules that said first communication is to be scanned on said first computer node;

forwarding said first communication to said first computer node without scanning said first communication for computer viruses, wherein said first computer node scans said first communication for computer viruses using said second virus scanner;

receiving a second communication at the firewall;

identifying a second set of attributes of said second communication;

determining from said second set of attributes and said rules that the firewall is responsible for scanning said first communication for computer viruses; and

operating said first virus scanner to scan said second communication for computer viruses."

The Examiner continues by stating that Segal inherently discloses a virus scanner, in view of the excerpt from Segal below:

> "The situation can be improved upon by providing a set of firewall-type commands that include lists of which nodes, sources, networks are allowed to use certain destinations. These commands can be utilized by filtering devices and/or security devices such as firewalls, ingress nodes, switches, which would be informed which destination nodes, addresses, ports, are permitted to which source nodes or networks. These filtering devices and/or security devices may be separate stand-alone components or their capability may be integrated into other, possibly already existing, devices." (col. 3, lines 35-45)

For the reasons set forth hereinabove with respect to Group #1, there is simply no mention of any sort of virus scanning in such excerpt.

Again, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #7: Claim 8

With respect to Group #7, the Examiner relies on the following excerpt from Segal to make a prior art showing of appellant's claimed "second subset of proxy rules for application by a proxy operating on the firewall to determine how to handle said communication."

> "The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 3, lines 1-15)

Such excerpt from Segal and the remaining Segal reference, however, makes no mention of the use of proxies, let alone "a second subset of proxy rules for application by a proxy operating on

the firewall to determine how to handle said communication" (emphasis added). Thus, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #8: Claim 12

With respect to Group #8, the Examiner relies on the following excerpt from Segal to make a prior art showing of appellant's claimed "establishing a secure connection between the firewall and said first node," "receiving at the firewall a proposed set of criteria for determining when said first node shall scan a communication instead of the firewall," and "determining whether said proposed set of criteria conflicts with said second subset of said scanning rules."

> "The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 3, lines 1-15)

Such excerpt from Segal and the remaining Segal reference, however, makes no mention of the use of "receiving at the firewall a proposed set of criteria for determining when said first node shall scan a communication instead of the firewall," and "determining whether said proposed set of criteria conflicts with said second subset of said scanning rules" (emphasis added). Thus, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

Group #9: Claim 22

With respect to Group #9, the Examiner relies on the following excerpts from Segal to make a prior art showing of appellant's claimed:

> "a first set of criteria to be applied for all nodes connected to said firewall and all communications received at said firewall to determine if a first communication received at said firewall for a first destination node connected to said firewall may be scanned for target content by said first destination node rather than said firewall; and
> a second set of criteria to be applied for a subset of said all communications to determine if said first communication may be scanned for said target content by said second destination node rather than said firewall;
> wherein said second set of criteria are applied by said first proxy module and said subset of all communications includes communications formatted according to a predetermined communication protocol; and
> wherein said first set of criteria is applied prior to said second set of criteria."

> "In accordance with the invention, the network 40 the units 43, 45, 46, 47, 49, and 50 each comprise a shared list setting forth a plurality of listed nodes and a set of access privileges for each listed node. Access privileges are the types of transmissions that a given node listed in the shared list is permitted to make. For example, consider the case where node B1 is a computer or LAN at an accounting firm. The firm may want to restrict the nodes from which it receives or transmits E-mail or certain types of transmissions (i.e. File Transfer Protocol (FTP). In this case, the firm wishes to receive e-mail only form its clients Z1, Y2, and X4. Node B1 would instruct node 45 to provide that the shared list residing at security node 45 would intercept all e-mail and only allow e-mail form nodes Z1, Y2 and X4 but in this distributed system, it is also possible for security node 49 to only allow e-mail from Y2, node 50 prohibits e-mail form Z2 and so forth. Thus, with the cooperation of other nodes, it is virtually impossible to overwhelm node 45 with unpermitted transmissions. The shared list may provide with respect to any listed node that it can only transmit to certain other listed nodes and, with respect to those nodes it can transmit to, restrictions applicable to such transmissions." (col. 2, line 60 - col. 3, line 15)

Simply nowhere in such excerpt from Segal is there any disclosure, teaching or even suggestion of any sort of "a first set of criteria to be applied for all nodes connected to said firewall and all communications received at said firewall ... a second set of criteria ... wherein said second set of criteria are applied by said first proxy module and said subset of all communications includes

communications formatted according to a predetermined communication protocol .... wherein said first set of criteria is applied **prior** to said second set of criteria."

Still yet, the foregoing anticipation criterion has simply not been met by Segal, with respect to the foregoing claim limitations.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

IX APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))

The text of the claims involved in the appeal is:

1. (Original) A method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content; and

forwarding said first communication to said first computer node;

wherein said first computer node receives and scans the communication for said target content.

2. (Original) The method of claim 1, further comprising:

receiving a second communication at the firewall, wherein said second communication is intended for a second computer node;

identifying one or more attributes of said second communication;

determining from said criteria and said attributes of said second communication whether said second computer node is permitted to scan said second communication for predetermined content;

scanning said second communication at the firewall for said predetermined content; and

forwarding said second communication to said second computer node;

wherein said second computer node receives but does not scan said second communication for said predetermined content.

3. (Original) The method of claim 2, further comprising marking said second communication before said forwarding to said second computer node.

4. (Original) The method of claim 1, wherein said partitioning comprises:

receiving scanning capabilities of a first computer node connected to the firewall;

consulting a set of scanning requirements specified by an operator of the firewall; and

specifying a set of criteria to identify when a communication may be scanned for target content by said first computer node.

5. (Original) The method of claim 4, wherein said partitioning further comprises receiving a set of proposed criteria from said first computer node.

6. (Original) The method of claim 1, wherein said determining comprises:

identifying whether said firewall is capable of scanning said first communication for target content;

determining whether said firewall is configured to share responsibility for scanning said communications with one or more of said plurality of computer nodes;

determining whether said first node is capable of scanning said first communication for said target content; and

determining whether said communication satisfies one or more criteria in said set of criteria.

7. (Original) A method of protecting a network of computer nodes from computer viruses, wherein the network of computer nodes is connected to a firewall, comprising:

maintaining a set of scanning rules for determining when a communication received at a firewall is to be scanned on the firewall and when said communication may be scanned by the destination node of said communication;

receiving a first communication at the firewall, wherein said first communication is intended for a first computer node connected to the firewall;

determining whether a first virus scanner is enabled on the firewall;

determining whether a second virus scanner is enabled on said first computer node;

identifying a first set of attributes of said first communication;

determining from said first set of attributes and said rules that said first communication is to be scanned on said first computer node;

forwarding said first communication to said first computer node without scanning said first communication for computer viruses, wherein said first computer node scans said first communication for computer viruses using said second virus scanner;

receiving a second communication at the firewall;

identifying a second set of attributes of said second communication;

determining from said second set of attributes and said rules that the firewall is responsible for scanning said first communication for computer viruses; and

operating said first virus scanner to scan said second communication for computer viruses.

8. (Original) The method of claim 7, wherein said set of scanning rules comprises:

a first subset of firewall rules for application by the firewall to determine how to handle said communication; and

a second subset of proxy rules for application by a proxy operating on the firewall to determine how to handle said communication.

9. (Original) The method of claim 7, wherein said set of scanning rules comprises:

a first subset of scanning rules for determining when said communication may be scanned for target content by a destination node of said communication instead of the firewall; and

a second subset of scanning rules for determining when said communication is to be scanned on said destination node and not on the firewall.

10. (Original) The method of claim 9, further comprising negotiating between the firewall and said first node to define said first subset of said scanning rules.

11. (Original) The method of claim 9, further comprising receiving said second subset of said scanning rules from a firewall administrator.

12. (Original) The method of claim 10, wherein said negotiating comprises:

establishing a secure connection between the firewall and said first node;

receiving at the firewall a proposed set of criteria for determining when said first node shall scan a communication instead of the firewall; and

determining whether said proposed set of criteria conflicts with said second subset of said scanning rules.

13. (Original) The method of claim 10, wherein said negotiating further comprises providing said first subset of said scanning rules to said first node.

14. (Original) The method of claim 10, wherein said negotiating further comprises sending an updated version of said second virus scanner to said first node.

15. (Original) The method of claim 10, wherein said negotiating is performed after said second virus scanner is configured on said first node by a user.

16. (Original) The method of claim 10, wherein said negotiating is performed after said first node is rebooted.

17. (Original) A computer readable storage medium storing instructions that, when executed by a computer, cause the computer to perform a method of scanning a communication received at a firewall for target content, wherein the communication is directed to one of a set of computer nodes connected to the firewall, the method comprising:

maintaining on the firewall a scanning module configured to scan communications received at the firewall;

maintaining a set of criteria for determining when one of said communications may be scanned at a computer node connected to the firewall instead of at the firewall;

partitioning responsibility for scanning said communications between said firewall and a first computer node connected to the firewall;

receiving a first communication at the firewall, wherein said first communication is intended for said first computer node;

identifying one or more attributes of said first communication;

determining from said criteria and said attributes whether to scan said first communication for target content on the firewall;

determining from said criteria and said attributes whether said first computer node is configured to scan said first communication for said target content; and

forwarding said first communication to said first computer node;

wherein said first computer node receives and scans the communication for said target content.

18. (Original) A computer readable storage medium containing a data structure configured to facilitate a determination as to whether a communication received at a firewall is to be scanned for target content on the firewall or on a destination node of the communication, the data structure comprising:

a first indicator configured to indicate whether a first communication scanning module is installed on a firewall;

a second indicator configured to indicate whether a second communication scanning module is installed on a destination node of a communication received at the firewall; and

a set of criteria to be applied to said communication to determine if said communication is to be scanned for target content at the firewall or at the destination node;

wherein said second indicator and said set of criteria are configured during a negotiation process between the firewall and the destination node.

19. (Original) An apparatus for scanning a communication received at a firewall to detect target content, wherein the communication is selectively scanned at one of the firewall and a destination node of the communication, comprising:

a firewall configured to receive a communication from an external entity for a first node connected to said firewall, said firewall comprising:

a first proxy module configured to establish a connection to the external entity;

a first scanning module configured to scan said communication for target content; and

a set of rules configured to determine whether said communication is to be scanned for said target content on said firewall or on the first node; and

a first computer node connected to the firewall and comprising a second scanning module, wherein said first computer node negotiates with said firewall to configure a first subset of said rules to identify when said first computer node shall scan said communication rather than said firewall;

wherein a measurement of performance of said firewall is increased as a result of said first node scanning one or more communications rather than said firewall.

20. (Original) The apparatus of claim 19, wherein said first node further comprises a negotiation module to negotiate with said firewall on behalf of multiple scanning modules, including said second scanning module.

21. (Original) The apparatus of claim 19, wherein said firewall further comprises a negotiation module to negotiate with said first node on behalf of multiple proxies, including said first proxy module.

22. (Original) The apparatus of claim 19, wherein said set of rules comprises:

a first set of criteria to be applied for all nodes connected to said firewall and all communications received at said firewall to determine if a first communication received at said firewall for a first

destination node connected to said firewall may be scanned for target content by said first destination node rather than said firewall; and

a second set of criteria to be applied for a subset of said all communications to determine if said first communication may be scanned for said target content by said second destination node rather than said firewall;

wherein said second set of criteria are applied by said first proxy module and said subset of all communications includes communications formatted according to a predetermined communication protocol; and

wherein said first set of criteria is applied prior to said second set of criteria.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P263/99.010.01).

Respectfully submitted,

By: _____ Date: 5/18/04

Kevin J. Zilka

Reg. No. 41,429

Silicon Valley IP Group, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660